REFERENCES

[1] S. Li, L. D. Xu, and S. Zhao, "The internet of things: a survey," *Inf. Syst. Front.*, vol. 17, no. 2, pp. 243–259, Apr. 2015.

[2] R. Ande, B. Adebisi, M. Hammoudeh, and J. Saleem, "Internet of things: Evolution and technologies from a security perspective," *Sustain. Cities Soc.*, vol. 54, no. 101728, p. 101728, Mar. 2020.

[3] A. Thakkar and R. Lohiya, "A review on machine learning and deep learning perspectives of IDS for IoT: Recent updates, security issues, and challenges," *Arch. Comput. Methods Eng.*, vol. 28, no. 4, pp. 3211–3243, Jun. 2021.

[4] J. Liu, K. Xiao, L. Luo, Y. Li, and L. Chen, "An intrusion detection system integrating network-level intrusion detection and host-level intrusion detection," in *2020 IEEE 20th International Conference on Software Quality, Reliability and Security (QRS)*, 2020, pp. 122–129.

[5] T. Radivilova, L. Kirichenko, A. S. Alghawli, A. Ilkov, M. Tawalbeh, and P. Zinchenko, "The complex method of intrusion detection based on anomaly detection and misuse detection," in *2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, 2020, pp. 133–137.

[6] N. Koroniotis, N. Moustafa, E. Sitnikova, and J. Slay, "Towards developing network forensic mechanism for botnet activities in the iot based on machine learning techniques," in *Mobile Networks and Management*, J. Hu, I. Khalil, Z. Tari, and S. Wen, Eds. Cham: Springer International Publishing, 2018, pp. 30–44.

[7] T. T. Bhavani, M. K. Rao, and A. M. Reddy, "Network intrusion detection system using random forest and decision tree machine learning techniques," in *First International Conference on Sustainable Technologies for Computational Intelligence*, A. K. Luhach, J. A. Kosa, R. C. Poonia, X.-Z. Gao, and D. Singh, Eds. Singapore: Springer Singapore, 2020, pp. 637–643.

[8] H. H. Pajouh, R. Javidan, R. Khayami, A. Dehghantanha, and K.-K. R. Choo, "A two-layer dimension reduction and two-tier classification model for

anomaly-based intrusion detection in iot backbone networks," *IEEE Transactions on Emerging Topics in Computing*, vol. 7, no. 2, pp. 314–323, 2019.

[9] S. Rachmadi, S. Mandala, and D. Oktaria, "Detection of dos attack using adaboost algorithm on iot system," in *2021 International Conference on Data Science and Its Applications (ICoDSA)*, 2021, pp. 28–33.

[10] C. Bentéjac, A. Csörgő, and G. Martínez-Muñoz, "A comparative analysis of gradient boosting algorithms," *Artif. Intell. Rev.*, vol. 54, no. 3, pp. 1937–1967, Mar. 2021.

[11] H. Binder, O. Gefeller, M. Schmid, and A. Mayr, "The evolution of boosting algorithms," *Methods Inf. Med.*, vol. 53, no. 06, pp. 419–427, 2014.

[12] A. A. Reyes, F. D. Vaca, G. A. Castro Aguayo, Q. Niyaz, and V. Devabhaktuni, "A machine learning based two-stage wi-fi network intrusion detection system," *Electronics*, vol. 9, no. 10, 2020. [Online]. Available: https://www.mdpi.com/2079-9292/9/10/1689

[13] B. A. Tama, L. Nkenyereye, S. R. Islam, and K.-S. Kwak, "An enhanced anomaly detection in web traffic using a stack of classifier ensemble," *IEEE Access*, vol. 8, pp. 24 120–24 134, 2020.

[14] E. Ashraf, N. F. F. Areed, H. Salem, E. H. Abdelhay, and A. Farouk, "FIDChain: Federated intrusion detection system for blockchain-enabled IoT healthcare applications," *Healthcare (Basel)*, vol. 10, no. 6, p. 1110, Jun. 2022.

[15] S. Dasari and R. Kaluri, "An effective classification of ddos attacks in a distributed network by adopting hierarchical machine learning and hyperparameters optimization techniques," *IEEE Access*, vol. 12, pp. 10 834–10 845, 2024.

[16] S. S. Panwar, Y. P. Raiwani, and L. S. Panwar, "Evaluation of network intrusion detection with features selection and machine learning algorithms on cicids-2017 dataset," *SSRN Electronic Journal*, 2019.

[17] S. S. Panwar, P. S. Negi, and Y. P. Raiwani, "Implementation of machine learning algorithms on CICIDS-2017 dataset for intrusion detection using WEKA," *International Journal of Recent Technology and Engineering (IJRTE)*, vol. 8, no. 3, pp. 2195–2207, sep 2019. [Online]. Available: https://doi.org/10.35940%2Fijrte.c4587.098319

[18] A. A. Laghari, K. Wu, R. A. Laghari, M. Ali, and A. A. Khan, "RETRACTED ARTICLE: A review and state of art of internet of things (IoT)," *Arch. Comput. Methods Eng.*, vol. 29, no. 3, pp. 1395–1413, May 2022.

[19] P. Malhotra, Y. Singh, P. Anand, D. K. Bangotra, P. K. Singh, and W.-C. Hong, "Internet of things: Evolution, concerns and security challenges," *Sensors*, vol. 21, no. 5, 2021. [Online]. Available: https://www.mdpi.com/1424-8220/21/5/1809

[20] B. H. Charlie Scott, Paul Wolfe, *Snort for Dummies*, ser. For dummies. Wiley Pub, 2004.

[21] H. C. T. Kwangjo Kim, Muhamad Erza Aminanto, *Network Intrusion Detection using Deep Learning*, 1st ed. Springer Singapore, 2018.

[22] S. Dhaliwal, A.-A. Nahid, and R. Abbas, "Effective intrusion detection system using XGBoost," *Information*, vol. 9, no. 7, p. 149, Jun. 2018. [Online]. Available: https://doi.org/10.3390/info9070149

[23] B. S. Bhati, G. Chugh, F. Al-Turjman, and N. S. Bhati, "An improved ensemble based intrusion detection technique using xgboost," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 6, p. e4076, 2021. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/ett.4076

[24] M. Zou, W.-G. Jiang, Q.-H. Qin, Y.-C. Liu, and M.-L. Li, "Optimized xgboost model with small dataset for predicting relative density of ti-6al-4v parts manufactured by selective laser melting," *Materials*, vol. 15, no. 15, 2022. [Online]. Available: https://www.mdpi.com/1996-1944/15/15/5298

[25] A. A. Ibrahim, R. L. Ridwan, M. M. Muhammed, R. O. Abdulaziz, and G. A. Saheed, "Comparison of the catboost classifier with other machine learning methods," *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 11, 2020. [Online]. Available: http://dx.doi.org/10.14569/IJACSA.2020.0111190

[26] W. Chang, X. Wang, J. Yang, and T. Qin, "An improved catboost-based classification model for ecological suitability of blueberries," *Sensors*, vol. 23, no. 4, 2023. [Online]. Available: https://www.mdpi.com/1424-8220/23/4/1811

[27] R. Zebari, A. Abdulazeez, D. Zeebaree, D. Zebari, and J. Saeed, "A comprehensive review of dimensionality reduction techniques for feature selection

and feature extraction," *Journal of Applied Science and Technology Trends*, vol. 1, no. 1, pp. 56–70, May 2020.

[28] F. Kherif and A. Latypova, "Chapter 12 - principal component analysis," in *Machine Learning*, A. Mechelli and S. Vieira, Eds. Academic Press, 2020, pp. 209–225. [Online]. Available: https://www.sciencedirect.com/science/article/pii/B9780128157398000122

[29] E. C. P. Neto, S. Dadkhah, R. Ferreira, A. Zohourian, R. Lu, and A. A. Ghorbani, "Ciciot2023: A real-time dataset and benchmark for large-scale attacks in iot environment," *Sensors*, vol. 23, no. 13, 2023. [Online]. Available: https://www.mdpi.com/1424-8220/23/13/5941

[30] M. H. Amrullah, F. Dewanta, and M. E. Aminanto, "Double layer machine learning for network intrusion detection system on web server," in *2023 10th International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE)*, 2023, pp. 281–286.

[31] A. R. M. A. Basher and S. J. Hallam, "Relabeling metabolic pathway data with groups to improve prediction outcomes," in *Computational Advances in Bio and Medical Sciences*, M. S. Bansal, I. Măndoiu, M. Moussa, M. Patterson, S. Rajasekaran, P. Skums, and A. Zelikovsky, Eds. Cham: Springer International Publishing, 2022, pp. 38–50.

[32] A. Maulana Ibrahimy, F. Dewanta, and M. Erza Aminanto, "Lightweight machine learning prediction algorithm for network attack on software defined network," in *2022 IEEE Asia Pacific Conference on Wireless and Mobile (APWiMob)*, 2022, pp. 1–6.

[33] M. Bach, A. Werner, and M. Palt, "The proposal of undersampling method for learning from imbalanced datasets," *Procedia Computer Science*, vol. 159, pp. 125–134, 2019. [Online]. Available: https://doi.org/10.1016%2Fj.procs.2019.09.167

[34] M. M. Ahsan, M. A. P. Mahmud, P. K. Saha, K. D. Gupta, and Z. Siddique, "Effect of data scaling methods on machine learning algorithms and model performance," *Technologies*, vol. 9, no. 3, 2021. [Online]. Available: https://www.mdpi.com/2227-7080/9/3/52

[35] J. Chu, T.-H. Lee, and A. Ullah, "Component-wise AdaBoost algorithms for high-dimensional binary classification and class probability prediction," in

Handbook of Statistics, ser. Handbook of statistics. Elsevier, 2020, pp. 81–114.